## CLAIMS

What is claimed is:

1. A method of controlling access to electronic information comprising the steps of providing:

at least one user apparatus;

a remote server;

a communications link between the at least one user apparatus and the remote server;

allocating disk storage space on the remote server unique to the at least one user apparatus;

allowing the at least one user access to the storage space via username and password login to the server and via secure encryption of data sent to or from the user apparatus from or to the server.

2. A method of controlling access to electronic information as claimed in claim 1, wherein the secure encryption comprises:

transactions between user and server being encrypted using SSL (Secure Socket Layer); and

transactions involving access to the storage space being further protected by a requirement for a user to present a digital certificate.

3. A method of controlling access to electronic information as claimed in claim 2, wherein the digital certificate is required whenever the user attempts to read or write from or to the storage space.

4. A method of controlling access to electronic information as claimed in claim 3, wherein data sent by a user apparatus is encrypted by public key in the case of SSL transactions and additionally by private key via presentation of a digital certificate in the case of accessing the data storage space.

5. A method of controlling access to electronic information as claimed in claim 4, wherein data received by the server is decrypted via private key in the case of SSL transactions and by public key in the case of digital certificate verification accessing the data storage space.

6. A method of controlling access to electronic information as claimed in claim 1, wherein the method further comprises the additional step of allowing at least one further user access to the data storage space.

7. A method of controlling access to electronic information as claimed in claim 6, wherein each said at least one further user is allowed access to the data storage space upon presentation of a further digital certificate.

8. A method of controlling access to electronic information as claimed in claim 7, wherein the further users access t the data storage space can be managed by the at least one user with regard to times and dates when the at least one further user can write to and/or read from the data storage space.

9. An electronic safety deposit system comprising:

at least one user appartus;

a remote server;

a communications link between the at least one user apparatus and the remote server;

disk storage space allocated on the remote server unique to the at least one user apparatus; and

means for allowing the at least one user access to the storage space via username and password login and via secure encryption of data sent to or from the user apparatus from or to the server.

10. A method of providing an account-based Internet/Intranet service which allows an at least one account holder to:

create at least one secure electronic deposit box on a centralised server in which a box or boxes can be stored documentation in a secure environment;

manage timeframes for invited participants to access said documentation and or for the Invited Participant to upload to the centralised server further documentation.

11. A method as claimed in claim 10, wherein the method further allows the at least one account holder to track activity relating to each said at least one electronic deposit box.

12. A secure electronic deposit or tender box system comprising an account-based Internet or Intranet server system with a worldwide Web (HTTP) interface for uploading and downloading documentation onto a centralised server in a secure environment, using digital certificates to ensure data confidentiality, data integrity, data authentication, non-repudiation and proof of origin and receipt.

13. A computer program product adapted for use in the method of any claims 1 to 8, 10 and 11.

14. A computer program product when used in the method of any of claims 1 to 8, 10 and 11.

15. A computer program adapted for implementation of the method of any of claims 1 to 8, 10 and 11.

16. A computer or computer network when loaded with the computer program of claim 15.